Privacy Policy COAST

In accordance with Art. 13 and 14 of the General Data Protection Regulation (GDPR), we, Hamburger Hafen und Logistik AG (hereinafter referred to as "HHLA", "we", "us") would like to inform you about the collection, processing, and use of personal data in the context of the use of the COAST online platform and the associated processing activities. We process personal data only in accordance with the applicable data protection regulations, which result from the GDPR and the Federal Data Protection Act (BDSG).

1. Controller

Hamburger Hafen und Logistik Aktiengesellschaft

Bei St. Annen 1

20457 Hamburg

You can contact our data protection officer at the above address or at datenschutz@hhla.de.

2. Purpose of processing when using COAST

With COAST, HHLA offers access to a convenient and protected dialogue and information platform for our contractual partners, which provides information on the status of each container on our facilities and provides various resources and information.

COAST provides secure, real-time access to data that is relevant to you and your business. When using COAST, we process your data for the following purposes:

Provision of information and resources: Your personal data will be processed to provide you with direct and unbureaucratic access to the information and other resources that are relevant to you.

Identity management in the context of IT security: This includes effective protection against unauthorised access to HHLA systems as well as effective protection against attacks on the company network. Personal data is processed to prevent third-party access, data leakage and harmful content (malware, computer viruses) as well as to protect and secure your data and the HHLA network.

3. Legal basis for the processing

We process your data only to the extent permitted by law (the provisions of the GDPR and the BDSG).

Art. 6(1)(b) GDPR: We process your personal data to fulfil contractual obligations to which we are subject.

Art. 6 (1) (c) in conjunction with Art. 32 GDPR: We are obliged to take appropriate measures to protect your personal data. This includes effective protection against attacks on the company network through the introduction of multi-factor authentication and the collection of login data as part of log files.

Art. 6(1)(f) GDPR: We also have a legitimate interest in the functioning and efficient provision of information and resources. HHLA has a legitimate interest in data processing, to avert potential damage through the assertion, defence and exercise of legal claims, to further develop internal processes and their structures, and to support our employees.

HHLA ensures that data processing based on legitimate interests always takes place in accordance with the legal requirements, that no conflicting legitimate interests and rights of the data subjects prevail.

4. Categories of data and personal data

e.g. user information, user group information, device information IP Address

Categories of Data	**Data**
User data	Name, telephone number, e-mail, company, department, time of last login, user ID, authorization, individual configuration of the system, set up on, set up by user
Technical login details	e.g. IP address: The IP address of the user at the time of login. This information can be used to monitor suspicious activity; Operating system: The operating system on which the user is running the browser; Device type / device ID: Information about the device on which the login takes place; Device information: Additional technical information about the device, e.g. device model, screen resolution; Geographic location: Rough indication of the geographic location based on the IP address; Timestamp: The date and time of the login

Audit logs / configuration protocols	Logs for important actions on the platform: read and edit
Reports	If users of the platform create a so-called report for themselves on certain information (evaluation on the Home Screen)
Password Self-service	User, password history, reset requests
Authentication information from Microsoft Azure AD	e.g. user information, group information of the user, device information

5. Confidentiality of data processing and disclosure to third parties

Your personal data will not be transferred to third parties for purposes other than those listed.

The recipients of the data are the responsible office and the employees entrusted with administration and maintenance of the System.

For user and identification management, data is transmitted to Microsoft Azure AD, a product of our processor Microsoft Ireland Operations Limited, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, Ireland, with which a data processing agreement has also been concluded including the EU Standard Contractual Clauses (SCC). The data transfer is carried out to ensure reliable authentication and authorization when accessing COAST. By using Azure AD as an identity management solution, we can efficiently control access to COAST and the data it contains, and significantly increase IT security. This technical measure protects your data by preventing potential unauthorized access, data leaks and cyberattacks that could compromise our company data and your personal data.

As a matter of principle, data is not processed outside the EU/EEA and is only possible if an adequate level of data protection is guaranteed, considering the applicable data protection laws.

6. Duration of data storage

Personal data is generally stored for as long as the controller has a legitimate interest or is required by law. If the underlying purposes no longer apply or any statutory retention and documentation obligations no longer apply, this data will be deleted in accordance with the statutory provisions.

We will delete your user data if the contractual relationship with HHLA is terminated, if your employer requests us to delete it or if you as a user request us to delete it, unless we are obliged to retain it for a longer period of time under Union or Member State law, or in order to perform a task that is in the public interest or is carried out in the exercise of official authority. In case of 3 months of inactivity of the user (no registration of the user), the user account will be blocked and deleted after 12 months after the user has been blocked. The user can create individual reports independently at any time and delete them.

Authentication logs (Microsoft Azure AD) and audit logs / configuration logs are automatically deleted or completely anonymized after 90 days at the latest.

Log files or technical login data and data in connection with the self-service password reset are automatically deleted after 2 years at the latest.

Certain legal or legal obligations may require personal data to be retained beyond the above periods. However, in such cases, the data will only be kept for the necessary duration and in accordance with applicable data protection laws.

7. Your Data Protection Rights

As a data subject, you have the right to information about the personal data concerning you and to rectification of inaccurate data or erasure if one of the reasons stated in Art. 17 GDPR applies, e.g. if the data is no longer required for the purposes pursued. You also have the right to restriction of processing if one of the conditions specified in Art. 18 GDPR applies and, in the cases specified in Art. 20 GDPR, the right to data portability. You can revoke any consent you have given in accordance with Art. 7 para. 3 GDPR or object to data processing in accordance with Art. 21 GDPR.

Every data subject has the right to lodge a complaint with a supervisory authority if he or she believes that the processing of data concerning him or her violates data protection regulations. In particular, the right to lodge a complaint may be exercised with a supervisory authority in the Member State of the domicile or place of work of the data subject or the place of the alleged infringement.

In Hamburg, the competent supervisory authority is:

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit der Freien und Hanse-stadt Hamburg, Ludwig-Erhard-Str 22, 20459 Hamburg, e-mail: mailbox@datenschutz.hamburg.de.

Contact the Data Protection Officer:

You also have the right to contact our data protection officer at any time (datenschutz@hhla.de).